REMARKS/ARGUMENTS

Reconsideration is respectfully requested.

Claims 1-12 are pending before this amendment. By the present amendment, claims 2 and 8 are canceled without prejudice and claims 1 and 7 are amended, where claim 7 has been amended to include the limitations of canceled claim 8 along with additional amendments. No new matter has been added.

In the office action (page 2), claim 2 stands objected to as containing informalities. In response the applicants have amended the claims based on the examiner's comments. Therefore, the applicants respectfully requested withdrawal of the above aforementioned objection.

103 Rejections

In the office action (page 3), claims 1, 3-5 and 7-11 stand rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent No. 6,807,553 (Oerlemans) in view of U.S. Patent No. 6,356,112 (Tran). The "et al." suffix is omitted from the Tran reference name.

In the office action (page 8), claims 6 and 12 stand rejected under 35 U.S.C. §103(a) as being obvious over Oerlemans in view of Tran, and further in view of U.S. Patent No. 5,001,361 (Tamamura). The "et al." suffix is omitted from the Tamamura reference name.

The applicants respectfully disagree.

RESPONSE TO 103 Rejections

The present invention relates to an apparatus and method for generating random numbers using digital logic. More specifically, the present invention provides an apparatus and method for easily generating digital random numbers with only digital logic while securing randomness that a physical random number generating apparatus can provide using an analog circuit. In the presently claimed invention, in order to generate completely random numbers using only a digital circuit, (i) random values are **directly** output to an **input logic circuit** when a combination of an output of a feedback unit of a linear feedback shift register (LFSR) also being **directly input to the same input logic circuit** and a random signal value is output from this input logic circuit such that this output signal is input the LFSR, and (ii) clocks contain a jitter and when values of clocks are changed is determined by the jitter contained in the clocks. Also, the presently claimed invention, discloses having a fixed value prevention circuit that generates a signal with a value that allows an output of the input logic circuit (i.e.; where the random values and the output of the feedback unit of a linear feedback shift register (LFSR) are both **directly input to the same input logic circuit along with the output from the fixed value prevention circuit**) to have a different value to a value of an output of the shift register and inputs the generated signal to the input logic circuit, when a logic value of the external signal is **equivalent** to all the bit values stored in the shift register. Claim 1 (and similarly claim 7) has been amended to clarify this above described aspect of the presently claimed invention, which recites inter alia:

> --a fixed value prevention circuit that generates a signal with a value that allows an output of the input logic circuit to have a different value to a value of an output of the shift register and **inputs the**

> **generated signal to the input logic circuit**, when a logic value of the external signal is equivalent to all the bit values stored in the shift register, **and wherein the external signal is directly connected to the input logic circuit**-- [**emphasis** added].

Support for the amendments can be found specification at least at page 8, line 24 to page 9, line 34 and FIG. 3.

Applicants respectfully submit that Oerlemans nor Tran nor Tamamura, neither alone nor in combination, discloses nor suggests the above-identified feature of claim 1 (and similarly claim 7). Specifically, Oerlemans is silent with respect to: a fixed value prevention circuit that generates a signal with a value that allows an output of the input logic circuit to have a different value to a value of an output of the shift register and inputs the generated signal to the input logic circuit, when a logic value of the external signal is equivalent to all the bit values stored in the shift register from **the external signal being directly connected to the input logic circuit**. Tran and/or Tamamura fail to cure this deficiency of Oerlemans.

In contrast, FIG. 2 of Oerlemans clearly discloses having a D type flip flop 2 receiving an input signal from the running oscillators 10, 20, and 30, where the D type flip flop receives an input from a system clock 3 **before** outputting a signal from the D type flip flop to the input logic XOR circuit 6. That is, Oerlemans can **not** disclose inputting an external signal directly to the XOR circuit 6 such that the generated external signal is **directly inputted to the XOR circuit 6** in combination with a **single** output of a feedback unit of a linear feedback shift register (LFSR) 4 being **directly input to the same XOR circuit 6 and the output from the NOR circuit 7, wherein** a random signal value is then output from this XOR circuit 6 as an input to the LFSR 4, which generates a signal with a value that **allows** an output of the XOR circuit 6 (i.e.; where the external signal and the output of the feedback unit of a linear feedback shift register (LFSR) are both **directly input to the same XOR circuit 6 along with the output form the NOR circuit 7 being inputted to the XOR circuit 6**) to have a different value to a value of an output of the shift register and inputs the generated signal to the input logic circuit, **when a logic value of the external signal is equivalent to all the bit values stored in the shift register** 4 (Oerlemans col. 3, line 60 to col. 4, line 21 and FIGs. 1 and 2).

In contradistinction, FIG. 3 of the presently claimed invention illustrates having a 4-bit LFSR that includes a fixed value prevention circuit 300 such that this fixed value prevention circuit 300 **prevents series generated by a shift register 100 from being unchanged in response to clock input** as follows:

> "an LFSR **according to the present invention generates random numbers by combining an output of a feedback circuit and an external signal**. Accordingly, when the value of the external signal is 1, all outputs of the first through fourth registers 110 through 140 may have values of 0 as shown in the series described with reference to FIG. 2. If the value of the external signal is changed and fixed to 0 when input of the external signal with random values makes all the outputs of the first through fourth registers 110 through 140 have a value of 0, the outputs of al the shift registers of the shift register 100 are fixed to 0 regardless of a value of an input clock. Similarly, if the value of the external signal is fixed to 1 when input of the external signal with random values makes all the outputs of the first through fourth registers 110 through 140 have a value of 1, the outputs of all the shift registers of the shift register 100 are fixed to 1 regardless of a value of an input clock. **Accordingly, the fixed value prevention circuit 300 is required to prevent values of outputs of the shift register 100 from being fixed to a particular value.**
>
> The fixed value prevention circuit 300 includes a first circuit 310 that inverts the outputs of the first through fourth registers 110 through 140 and the value of the external signal and performs an AND operation on the inversion results, or performs an OR operation on the outputs of the first through fourth registers 110 through 140 and inverts the OR operation result; a second circuit 320 that performs an AND operation on the outputs of the first through fourth registers 110 through 140 and the external signal value; and a third circuit 330 that performs an OR operation on outputs of the first and second circuits 310 and 320. An input logic circuit 500 combines the output of the third circuit 330, the external signal value, and

> the output of the feedback circuit 200, and inputs the result of combination to the shift register 100, thereby preventing outputs of the shift register 100 from being fixed to a particular value.
>
> When the outputs of the first through fourth registers 110 through 140 have a value of 0000 and the external signal has a value of 0, an output of the feedback circuit 200 has a value of 0 without the fixed value prevention circuit 300. In this case, a sum of the output of the feedback circuit 200 and the external signal value input to the shift register 100 is also 0, and therefore, values of outputs of the shift register 100 are fixed to 0000. **However, when the fixed value prevention circuit 300 Is installed, the first circuit 310 inverts the outputs of the first through fourth registers 110 through 140 and the external signal value, performs an AND operation on a result of inversion, and generates a signal with a value of 1**. When the signal with the value of 1 is input to the third circuit 330, the third circuit 330 also generates a signal with a value of 1. That is, the fixed value prevention circuit 300 outputs a signal with a value of 1. The value of the signal output from the fixed value prevention circuit 300, the external signal value, and a value of the output of the feedback circuit 200 are combined by the input logic circuit 500, thus obtaining a value of 1. **The value of 1 output from the input logic circuit 500 is input to the shift register 100. In this case, the next values output from the first through fourth shift registers 110 through 140 are 1000 in response to clock input. Accordingly, it is possible to prevent the output values of the shift register 100 from being fixed to 0000 using the fixed value prevention circuit 300"**,

(specification page 8, line 24 to page 9, line 34 and FIG. 3).

As described above, the presently claimed invention **discloses being able to randomly generate every possible complete random number that can be statistically generated according to a bit value, only using digital logic**.

Also, an apparatus for generating random numbers according to the present invention is capable of easily generating random numbers using **only** digital logic, without an analog circuit and a complicated algorithm. Further, the claimed digital logic can be fabricated as a compact unit for reducing power consumption. Thus, the present invention is embodied as a system-on-chip random number generation apparatus, such as an integrated circuit (IC) card, that does not occupy a large space and saves power.

Also, the present invention is easy to manufacture like a conventional pseudo random number generating apparatus, and thus applicable to various types of systems..

Therefore, the applicants respectfully submit that Oerlemans, Tran, or Tamamura, alone or in combination, fails to disclose or suggest each and every limitation of independent claim 1 (and similarly claim 7) of the presently claimed invention which recites: --a fixed value prevention circuit that generates a signal with a value that allows an output of the input logic circuit to have a different value to a value of an output of the shift register and **inputs the generated signal to the input logic circuit**, when a logic value of the external signal is equivalent to all the bit values stored in the shift register, and wherein the external signal is directly connected to the input logic circuit-- [**emphasis** added]. Thus, the applicant respectfully submits that claim 1 (and similarly clam 7) is in condition for allowance over the examiner's cited references.

DEPENDENT CLAIMS

The other claims are dependent from either independent claim 1 or independent claim 7 and are therefore believed patentable for at least the same reasons discussed above for claim 1. Therefore, each dependent claim is also deemed to define an additional aspect of the invention. However, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

For the reasons set forth above, the applicants respectfully submit that claims 1-12, now pending in this application, are in condition for allowance over the cited references. Accordingly, the applicants respectfully request reconsideration and withdrawal of the outstanding rejections and earnestly solicit an indication of allowable subject matter.

This amendment is considered to be responsive to all points raised in the office action. Should the examiner have any remaining questions or concerns, the examiner is encouraged to contact the undersigned attorney by telephone to expeditiously resolve such concerns.

Respectfully submitted,

Dated: June 24, 2010

Keith S. Van Duyne

Keith S. Van Duyne, Reg. No. 54,505
Ladas & Parry LLP
224 South Michigan Avenue
Chicago, Illinois 60604
(312) 427-1300